

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2002-175084  
(P2002-175084A)

(43)公開日 平成14年6月21日(2002.6.21)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 1 0 K 15/02		G 1 0 K 15/02	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 C 0 6 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 A 5 J 1 0 4
G 1 0 L 19/00		H 0 4 M 1/00	U 5 K 0 2 7
H 0 4 L 9/08		11/00	3 0 2 5 K 1 0 1

審査請求 未請求 請求項の数9 O L (全 28 頁) 最終頁に続く

(21)出願番号	特願2000-372418(P2000-372418)	(71)出願人	000001889 三洋電機株式会社 大阪府守口市京阪本通2丁目5番5号
(22)出願日	平成12年12月7日(2000.12.7)	(72)発明者	堀 吉宏 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内
		(72)発明者	上村 透 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内
		(74)代理人	100064746 弁理士 深見 久郎 (外3名)

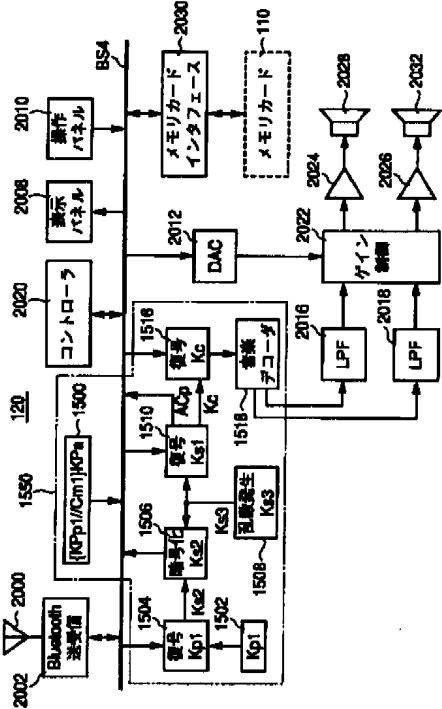
最終頁に続く

(54)【発明の名称】 再生装置

(57)【要約】

【課題】 暗号化コンテンツデータを通常のコンテンツデータと同じように再生可能な再生装置を提供する。

【解決手段】 ポータブルステレオ120は、コンテンツ再生デバイス1550を含む。コントローラ2020は、アンテナ2000および送受信部2002を介して携帯電話機に装着されたメモ리카ードから暗号化コンテンツデータおよびライセンスを受信して暗号化コンテンツデータおよびライセンスをコンテンツ再生デバイス1550に与える。コンテンツ再生デバイス1550は、ライセンスによって暗号化コンテンツデータを復号し、かつ、再生してLPF2016、2018へ出力する。そして、音楽データは、LPF2016、2018、ゲイン制御部2022、増幅器2024、2026、スピーカ2028、2032を経て外部へ出力される。



(2)

特開 2002-175084

1

## 【特許請求の範囲】

【請求項 1】 暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスとを格納したデータ記録装置が装着された端末通信装置から前記暗号化コンテンツデータおよび前記ライセンスを受信し、その受信した暗号化コンテンツデータを前記ライセンスによって再生する再生装置であって、前記端末通信装置との間でデータの送受信を行なう専用送受信部と、指示を入力するための操作部と、前記暗号化コンテンツデータを前記ライセンスによって再生するコンテンツ再生部と、前記コンテンツ再生部によって再生されたコンテンツデータを外部へ出力するための出力部と、制御部とを備え、前記制御部は、前記操作部から入力された暗号化コンテンツデータの再生指示に応じて、前記専用送受信部を介して前記端末通信装置へアクセスし、前記端末通信装置によって前記データ記録装置から読出された暗号化コンテンツデータおよびライセンスを前記専用送受信部を介して受信し、その受信した暗号化コンテンツデータおよびライセンスを前記コンテンツ再生部へ与える、再生装置。

【請求項 2】 前記端末通信装置の電源部を充電するための充電部をさらに備える、請求項 1 に記載の再生装置。

【請求項 3】 前記端末通信装置を介して通話するためのハンドフリーな通話部をさらに備える、請求項 1 に記載の再生装置。

【請求項 4】 前記通話部は、ユーザの音声を入力するための入力部と、通話相手の音声を外部へ出力するための音声出力部と、前記専用送受信部からの前記通話相手の音声信号を復号し、その復号した音声を前記音声出力部に与え、前記入力部からの音声を所定の方式に符号化し、その符号化した音声信号を前記専用送受信部に与える復号／符号部とを含む、請求項 3 に記載の再生装置。

【請求項 5】 前記データ記録装置を装着するための装着部と、前記データ記録装置との間でデータの授受を制御するためのインタフェースとをさらに備え、前記装着部に前記データ記録装置が装着されたとき、前記制御部は、前記操作部から入力された暗号化コンテンツデータの再生指示に応じて、前記インタフェースを介して前記データ記録装置から暗号化コンテンツデータおよびライセンスを取得し、その取得した暗号化コンテンツデータおよびライセンスを前記コンテンツ再生部へ与える、請求項 1 から請求項 4 のいずれか 1 項に記載の再生装置。

【請求項 6】 前記コンテンツ再生部は、前記データ記

2

録装置に対する認証データを保持する認証データ保持部を含み、

前記制御部は、前記認証データを前記専用送受信部を介して前記端末通信装置へ送信し、前記データ記録装置において前記認証データが認証されると、前記専用送受信部を介して前記暗号化コンテンツデータおよび前記ライセンスを受信する、請求項 1 から請求項 4 のいずれか 1 項に記載の再生装置。

【請求項 7】 前記コンテンツ再生部は、

10 第 1 の共通鍵を発生する共通鍵発生部と、

前記第 1 の共通鍵による復号処理を行なう復号処理部と、

前記データ記録装置において発生された第 2 の共通鍵によって前記第 1 の共通鍵を暗号化する暗号処理部とをさらに含み、

前記制御部は、前記第 2 の共通鍵によって暗号化された第 1 の共通鍵を前記専用送受信部を介して前記端末通信装置へ送信し、前記端末通信装置から前記第 1 の共通鍵によって暗号化されたライセンス鍵を受信して前記コンテンツ再生部に与える、請求項 6 に記載の再生装置。

20

【請求項 8】 前記コンテンツ再生部は、前記データ記録装置に対する認証データを保持する認証データ保持部を含み、

前記制御部は、前記データ記録装置が前記端末通信装置に装着された場合、前記認証データを、前記専用送受信部を介して前記端末通信装置へ送信し、前記専用送受信部を介して、少なくとも前記ライセンスを受信し、前記データ記録装置が前記装着部に装着された場合、前記インタフェースを介して前記認証データを前記データ記録装置に与え、前記データ記録装置において前記認証データが認証されると、前記インタフェースを介して、前記ライセンスと前記暗号化コンテンツデータとを受信する、請求項 5 に記載の再生装置。

30

【請求項 9】 前記コンテンツ再生部は、

第 1 の共通鍵を発生する共通鍵発生部と、

前記第 1 の共通鍵による復号処理を行なう復号処理部と、

前記データ記録装置において発生された第 2 の共通鍵によって前記第 1 の共通鍵を暗号化する暗号処理部とをさらに含み、

前記制御部は、前記データ記録装置が前記端末通信装置に装着された場合、前記第 2 の共通鍵によって暗号化された第 1 の共通鍵を前記専用送受信部を介して前記端末通信装置へ送信し、前記端末通信装置から前記第 1 の共通鍵によって暗号化されたライセンスを受信して前記コンテンツ再生部に与え、前記データ記録装置が前記装着部に装着された場合、前記第 2 の共通鍵によって暗号化された第 1 の共通鍵を、前記インタフェース部を介して前記データ記録装置へ与え、前記データ記録装置から前記第 1 の共通鍵によって暗号化されたライセンスを受信

40

50

## 3

して前記コンテンツ再生部に与える、請求項8に記載の再生装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられる再生装置に関するものである。

## 【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が

## (3)

特開2002-175084

## 4

講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

## 【0014】

【発明が解決しようとする課題】しかし、携帯電話機以外に、暗号化コンテンツデータを再生する機能を持つ再生装置がないため、通常の音楽データとともに暗号化コンテンツデータを再生できないという問題がある。

【0015】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、暗号化コンテンツデータを通常のコンテンツデータと同じように再生可能な再生装置を提供することである。

## 【0016】

【課題を解決するための手段および発明の効果】この発明による再生装置は、暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスとを格納したデータ記録装置が装着された端末通信装置から暗号

## 5

化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータをライセンスによって再生する再生装置であって、端末通信装置との間でデータの送受信を行なう専用送受信部と、指示を入力するための操作部と、暗号化コンテンツデータをライセンスによって再生するコンテンツ再生部と、コンテンツ再生部によって再生されたコンテンツデータを外部へ出力するための出力部と、制御部とを備え、制御部は、操作部から入力された暗号化コンテンツデータの再生指示に応じて、専用送受信部を介して端末通信装置へアクセスし、

端末通信装置によってデータ記録装置から読出された暗号化コンテンツデータおよびライセンスを専用送受信部を介して受信し、その受信した暗号化コンテンツデータおよびライセンスをコンテンツ再生部へ与える。

【0017】この発明による再生装置においては、端末通信装置との間でデータのやり取りを通信によって行ない、端末通信装置に装着されたデータ記録装置から暗号化コンテンツデータおよびライセンスを受信し、暗号化コンテンツデータを再生する。

【0018】したがって、この発明によれば、暗号化コンテンツデータを、直接、取得することができない再生装置においても、暗号化コンテンツデータを再生することができる。

【0019】好ましくは、再生装置は、端末通信装置の電源部を充電するための充電部をさらに備える。

【0020】再生装置は、端末通信装置が装着されると、端末通信装置の電源部を充電する。

【0021】したがって、この発明によれば、再生装置は暗号化コンテンツデータをデータ記録装置から受信するのに必要な端末通信装置と一体化できる。

【0022】好ましくは、再生装置は、端末通信装置を介して通話するためのハンドフリーな通話部をさらに備える。

【0023】入力されたユーザの音声は通話部によって所定の符号化を施され、専用送受信部を介して端末通信装置へ送信され、端末通信装置からの音声信号は通話部によって復号され再生装置のユーザに与えられる。

【0024】したがって、この発明によれば、ユーザは、暗号化コンテンツデータを再生できるとともに、通話部を介して他の人とも通話ができる。

【0025】好ましくは、再生装置の通話部は、ユーザの音声を入力するための入力部と、通話相手の音声を外部へ出力するための音声出力部と、専用送受信部からの通話相手の音声信号を復号し、その復号した音声を音声出力部に与え、入力部からの音声を所定の方式に符号化し、その符号化した音声信号を専用送受信部に与える復号／符号部とを含む。

【0026】通話部は、音声を音声信号へ符号化し、音声信号を音声に復号する。したがって、この発明によれば、ユーザは、暗号化コンテンツデータを再生できると

## (4)

特開2002-175084

## 6

ともに、通話部を介して他の人とも通話ができる。

【0027】好ましくは、再生装置は、データ記録装置を装着するための装着部と、データ記録装置との間でデータの授受を制御するためのインタフェースとをさらに備え、装着部に前記データ記録装置が装着されたとき、制御部は、操作部から入力された暗号化コンテンツデータの再生指示に応じて、インタフェースを介してデータ記録装置から暗号化コンテンツデータおよびライセンスを取得し、その取得した暗号化コンテンツデータおよび

ライセンスをコンテンツ再生部へ与える。

【0028】再生装置は、装着されたデータ記録装置から暗号化コンテンツデータとライセンスとを取得し、その取得した暗号化コンテンツデータをライセンスによって再生する。

【0029】したがって、この発明によれば、他の装置に装着することによって暗号化コンテンツデータおよびライセンスを取得したデータ記録装置を装着して暗号化コンテンツデータを再生できる。

【0030】好ましくは、再生装置のコンテンツ再生部は、データ記録装置に対する認証データを保持する認証データ保持部を含み、制御部は、認証データを専用送受信部を介して端末通信装置へ送信し、データ記録装置において認証データが認証されると、専用送受信部を介して暗号化コンテンツデータおよびライセンスを受信する。

【0031】再生装置は、コンテンツ再生部が正規の機器であることが認証されると、暗号化コンテンツデータとライセンスとを受信する。そして、コンテンツ再生部は、暗号化コンテンツデータをライセンスによって再生する。

【0032】したがって、この発明によれば、不正な暗号化コンテンツデータの再生を防止できる。

【0033】好ましくは、再生装置のコンテンツ再生部は、第1の共通鍵を発生する共通鍵発生部と、第1の共通鍵による復号処理を行なう復号処理部と、データ記録装置において発生された第2の共通鍵によって第1の共通鍵を暗号化する暗号処理部とをさらに含み、制御部は、第2の共通鍵によって暗号化された第1の共通鍵を専用送受信部を介して端末通信装置へ送信し、端末通信装置から第1の共通鍵によって暗号化されたライセンス鍵を受信してコンテンツ再生部に与える。

【0034】コンテンツ再生部とデータ記録装置との間で、相互に発生させた共通鍵をやり取りすることによって安全な暗号化通信路を確保して、コンテンツ再生部は自己が発生した共通鍵によって暗号化されたライセンス鍵を受信する。

【0035】したがって、この発明によれば、より安全に暗号化コンテンツデータを再生できる。

【0036】好ましくは、再生装置のコンテンツ再生部は、データ記録装置に対する認証データを保持する認証

## 7

データ保持部を含み、制御部は、データ記録装置が端末通信装置に装着された場合、認証データを、専用送受信部を介して端末通信装置へ送信し、専用送受信部を介して、少なくともライセンスを受信し、データ記録装置が装着部に装着された場合、インタフェースを介して認証データをデータ記録装置に与え、データ記録装置において認証データが認証されると、インタフェースを介して、ライセンスと暗号化コンテンツデータとを受信する。

【0037】再生装置のコンテンツ再生部は、データ記録装置に対する認証データが認証されると、データ記録装置からライセンスと暗号化コンテンツデータとを受信し、ライセンスによって暗号化コンテンツデータを再生する。

【0038】したがって、この発明によれば、正規のコンテンツ再生部を有する再生装置だけがデータ記録装置から暗号化コンテンツデータとライセンスとを受信し、暗号化コンテンツデータを再生できる。

【0039】好ましくは、再生装置のコンテンツ再生部は、第1の共通鍵を発生する共通鍵発生部と、第1の共通鍵による復号処理を行なう復号処理部と、データ記録装置において発生された第2の共通鍵によって第1の共通鍵を暗号化する暗号処理部とをさらに含み、制御部は、データ記録装置が端末通信装置に装着された場合、第2の共通鍵によって暗号化された第1の共通鍵を専用送受信部を介して端末通信装置へ送信し、端末通信装置から第1の共通鍵によって暗号化されたライセンスを受信してコンテンツ再生部に与え、データ記録装置が装着部に装着された場合、第2の共通鍵によって暗号化された第1の共通鍵を、インタフェース部を介してデータ記録装置へ与え、データ記録装置から第1の共通鍵によって暗号化されたライセンスを受信してコンテンツ再生部に与える。

【0040】再生装置は、データ記録装置との間で共通鍵による相互認証を行ない、相互に認証された場合にデータ記録装置からライセンスを受信する。

【0041】したがって、この発明によれば、暗号化コンテンツデータを再生するライセンスをデータ記録装置から再生装置へより安全に送信できる。

【0042】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0043】図1は、本発明による再生装置（カーステレオまたはコンポーネントステレオ）が再生の対象とする暗号化コンテンツデータを通信機能を有する通信装置に配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0044】なお、以下では携帯電話網を介して音楽データを各携帯電話機に配信するデータ配信システムの構

## 8

成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ、教材データ、テキストデータ、朗読（音声）データ、ゲームプログラム等を配信する場合においても適用することが可能なものである。また、インターネット網や直接ダイヤルアップ接続による公衆電話網への適用も可能である。

【0045】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、各携帯電話機からの配信要求（配信リクエスト）を配信サーバ10に中継する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【0046】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0047】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0048】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0049】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0050】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0051】暗号化コンテンツデータおよびライセンス

を受信したメモリカード110は、カーステレオまたはコンポーネントステレオ等のポータブルステレオ120からの暗号化コンテンツデータの再生許諾要求に応じて、ポータブルステレオ120に内蔵されたコンテンツ再生デバイス（図示せず）の正当性を認証データに基づいて確認し、ライセンスを、携帯電話機100を介して通信によってポータブルステレオ120へ送信する。次いで、ポータブルステレオ120からの暗号化コンテンツデータの送信要求に対して、暗号化コンテンツデータを、携帯電話機100を介して通信によってポータブルステレオ120へ送信する。そして、ポータブルステレオ120は、暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスによって暗号化コンテンツデータを再生する。

【0052】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機またはポータブルステレオのユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第2には、通信においてライセンスを安全に配信するための方式であり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツ保護を実現する構成である。

【0053】なお、以下の説明においては、配信サーバ10から、各携帯電話機に暗号化コンテンツデータおよびライセンスを伝送する処理を「配信」と称することとする。

【0054】本発明の実施の形態においては、特に、配信、および再生において、これらのライセンスの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られたような不正な記録装置および再生装置（コンテンツを再生できるコンテンツ再生デバイスを備えた再生装置、必要に応じてポータブルステレオまたは携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0055】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0056】まず、配信サーバ10より配信されるデータについて説明する。コンテンツデータDcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcがこの形式で配信サーバ10より携帯電話ユーザに配布される。

【0057】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0058】さらに、配信サーバ10からは、暗号化コ

ンテンツデータとともに、コンテンツデータに関する情報あるいはサーバのアクセスに関する情報等を含む平文情報としての付加情報Dc-infが配布される。また、配信サーバ10からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ10と携帯電話機100との間でやり取りされる。さらに、コンテンツデータDcを識別するためのコードであるコンテンツIDおよび著作権者の許可範囲内において、利用者側からの指示であり、ライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する条件を示すアクセス制限ACmおよびデータ再生端末における再生条件を示す制御情報である再生制限ACpが存在する。具体的には、アクセス制限ACmはメモリカードからのライセンスまたはライセンス鍵を外部に出力に対するにあたっての制限情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生の特殊再生や期間を制限する制限情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0059】以後、トランザクションIDとコンテンツIDとを併せてライセンスIDと総称し、ライセンス鍵KcとライセンスIDとアクセス制限ACmと再生制限ACpとを併せて、ライセンスと総称することとする。

【0060】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機またはポータブルステレオのクラスごとに、コンテンツデータの配信、および再生を禁止することができるように証明書失効リストCRL（Certification Revocation List）の運用を行なう。以下では、必要に応じて記号CRLによって証明書失効リスト内のデータを表わすこともある。

【0061】証明書失効リスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機、メモリカード、およびコンテンツ再生デバイスのクラス証明書をリストアップした証明書失効リストデータCRLが含まれる。

【0062】証明書失効リストデータCRLは、配信サーバ10内で管理されるとともに、メモリカードにも記録保持される。このような証明書失効リストは、随時、更新していく必要があるが、データの変更については、基本的にはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から証明書失効リストの更新日時を判断し、更新されていないとき、新しい証明書失効リストを携帯電話機に配信する。また、証明書失効リストの変更については、変更点のみを反映した差分

10

20

30

40

50

データである差分CRLを配信サーバ10側より発生して、これに応じてメモリカードの証明書失効リストCRLが書替えられる構成とするも可能である。また、証明書失効リストの更新日時については、メモリカード側より出力し、これを配信サーバ10側で確認することによって更新日時の管理を実行する。差分CRLには更新日時CRLdateも含まれる。

【0063】このように、証明書失効リストCRLを、配信サーバのみならずメモリカードにおいても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードまたはコンテンツ再生デバイスの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードまたはコンテンツ再生デバイスへのライセンス鍵の供給を禁止する。このため、携帯電話機またはコンテンツ再生デバイスではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。クラスについては、後ほど詳細に説明する。

【0064】このように、メモリカードの証明書失効リストCRLは配信時に逐次データを更新する構成とする。また、メモリカードにおける証明書失効リストCRLの管理は、上位レベルとは独立にメモリカードでタンパーレジスタントモジュール(Tamper Resistant Module)に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから証明書失効リストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0065】図3は、図1に示すデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

【0066】メモリカード、およびコンテンツ再生デバイスには固有の公開暗号鍵KPyおよびKPMwがそれぞれ設けられ、公開暗号鍵KPyおよびKPMwは携帯電話機に固有の秘密復号鍵Kpおよびメモリカードに固有の秘密復号鍵Kmによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機、およびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、クラス鍵を共有する単位をクラスと称する。

【0067】また、コンテンツ再生デバイスのクラス証明書としてCpyが設けられ、メモリカードのクラス証明書としてCmwが設けられる。これらのクラス証明書は、コンテンツ再生デバイス、およびメモリカードのクラスごと、すなわちクラス鍵単位に異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、証明書失効リストにリストアップされてライセンス発行の禁止対象となる。

【0068】これらのコンテンツ再生デバイス、およびメモリカードに固有の公開暗号鍵およびクラス証明書は、認証データ{KPy//Cpy}KPaの形式または認証データ{KPMw//Cmw}KPaの形式で、出荷時にデータ再生デバイス、およびメモリカードにそれぞれ記録される。KPaは配信システム全体で共通の公開認証鍵であり、認証データを復号することで、その正当性を確認することができる。公開認証鍵KPaは、配信サーバ10およびメモリカード110内に保持される。

【0069】また、メモリカード110のデータ処理を管理するための鍵として、メモリカードという媒体ごとに個別に設定される公開暗号鍵KPMcxと、公開暗号鍵KPMcxで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Kmcxが存在する。

【0070】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ10、メモリカード110、コンテンツ再生デバイス(携帯電話機100、ポータブルステレオ120)において生成される共通鍵Ks1~Ks3が用いられる。

【0071】ここで、共通鍵Ks1~Ks3は、配信サーバ、コンテンツ再生デバイスもしくはメモリカードもしくはコンテンツ再生デバイス間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1~Ks3を「セッションキー」とも呼ぶこととする。

【0072】これらのセッションキーKs1~Ks3は、各通信セッションごとに固有の値を有することにより、配信サーバ、メモリカード、およびコンテンツ再生デバイスによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーKs3は、コンテンツ再生デバイスにおいて再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0073】図4は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、暗号化コンテンツデータのコンテンツID等の配信情報を保持するための情報データベース304と、パーソナルコンピュータの各ユーザごとにライセンス鍵等へのアクセス開始に従った課金情報を保持するための課金データベース302と、証明書失効リストCRLを管理するC

RLデータベース306と、情報データベース304に保持されたライセンスによって再生されるコンテンツデータのメニューを保持するメニューデータベース307と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションID等を含む、配信のログを保持する配信記録データベース308と、情報データベース304、課金データベース302、CRLデータベース306、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0074】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、携帯電話機100から送られてきた認証のためのメモリカード110の認証データ{Kpmw/Cmw}KPaを復号するための公開認証鍵KPaを保持する認証鍵保持部313と、送られてきた認証のための認証データ{Kpmw/Cmw}KPaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPaによって復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られた公開暗号鍵Kpmcxを用いて暗号化して、バスBS1に出力するための暗号処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0075】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制限ACmを、復号処理部320によって得られたメモリカードに固有の公開暗号鍵Kpmwによって暗号化するための暗号処理部326と、暗号処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号処理部328とを含む。

【0076】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0077】図5は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0078】携帯電話機100は、携帯電話機100の各部のデータ授受を行なうためのバスBS2と、携帯電話網により無線伝送される信号を受信するためのアンテナ1101と、アンテナ1101からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデ

ータを変調してアンテナ1101に与えるための送受信部1102と、ポータブルステレオ120からの信号を受信するためのアンテナ1103と、アンテナ1103からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機100からのデータを変調してアンテナ1103に与えるための送受信部1104と、バスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106と、外部からの指示を携帯電話機100に与えるための操作パネル1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるための表示パネル1110とを含む。

【0079】携帯電話機100は、さらに、配信サーバ10からのコンテンツデータ（音楽データ）を記憶しつつ復号化処理するための着脱可能なメモリカード110と、メモリカード110とバスBS2との間のデータの授受を制御するためのメモリインタフェース1200とを含む。

【0080】携帯電話機100は、さらに、携帯電話機（コンテンツ再生デバイス）の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵Kpp2およびクラス証明書Cp2を公開復号鍵KPaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kpp2/Cp2}KPaを保持する認証データ保持部1500を含む。ここで、携帯電話機（データ端末装置）100のクラスyは、y=2であるとする。

【0081】携帯電話機100は、さらに、携帯電話機（コンテンツ再生デバイス）固有の復号鍵であるKp2を保持するKp保持部1502と、バスBS2から受けたデータをKp2によって復号しメモリカード110によって発生されたセッションキーKs2を得る復号処理部1504とを含む。

【0082】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵Kcおよび再生制限ACpを受取る際に、セッションキー発生部1508により発生されたセッションキーKs3を復号処理部1504によって得られたセッションキーKs2によって暗号化しバスBS3に出力する暗号処理部1506とを含む。

【0083】携帯電話機100は、さらに、バスBS2上のデータをセッションキーKs3によって復号して出力する復号処理部1510と、バスBS2より暗号化コンテンツデータ{Dc}Kcを受けて、復号処理部1510より取得したライセンス鍵Kcによって復号しコンテンツデータを出力する復号処理部1516と、復号処理部1516の出力を受けてコンテンツデータDcを再



15

生するための音楽デコーダ1518と、混合器1118の出力を外部出力装置（図示省略）へ出力するための端子1120とを含む。

【0084】携帯電話機100は、さらに、ユーザの音声を入力するためのマイク1114と、マイク1114からの音声を符号化してバスBS2に与え、またはバスBS2上の音声信号を復号してスピーカ1116に与える音声処理部1112と、音声処理部1112部からの音声信号を外部へ出力するためのスピーカ1116と、音声処理部1112からの音声信号または音楽デコーダ1518からの音楽信号を混合して端子1120へ出力するための混合器1118とを含む。

【0085】なお、図5においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス1550を構成する。また、図5においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0086】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0087】図6は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有のクラス鍵である公開暗号鍵および秘密復号鍵として、K P m wおよびK m wが設けられ、メモリカードのクラス証明書C m wが設けられるが、メモリカード110においては、これらはクラスwは、w=7で表わされるものとする。また、メモリカードごとに個別に設けられる個別なメモリカードを識別する識別子xは、x=8で表されるものとする。

【0088】したがって、メモリカード110は、認証データ{K P m 7 / C m 7} K P aを保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵であるK m c 8を保持するK m c 保持部1402と、メモリカードの種類ごとに設定される固有の秘密復号鍵K m 7を保持するK m 保持部1421と、K m c 8によって復号可能な公開暗号鍵K P m c 8を保持するK P m c 保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵K P m 7およびクラス証明書C m 7を公開認証鍵K P aで復号することでその正当性を認証できる状態に暗号化した認証データ{K P m 7 / C m 7} K P aとして保持する。

【0089】このように、メモリカードという記録装置に固有の暗号鍵および復号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

(9)

特開2002-175084

16

【0090】メモリカード110は、さらに、メモリインタフェース1200との間で信号を、端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS4と、バスBS4にインタフェース1424から与えられるデータから、メモリカードのクラスごとに固有の秘密復号鍵K m 7をK m 保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーK s 1を接点P aに出力する復号処理部1422

10 と、K P a 保持部1414から認証鍵K P aを受けて、バスBS4に与えられるデータからK P aによる復号処理を実行して復号結果を暗号処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS4に出力する暗号処理部1406とを含む。

【0091】メモリカード110は、さらに、再生セッションにおいてセッションキーK s 2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーK s 2を復号処理部1408によって得られるコンテンツ再生デバイスのクラス鍵である公開暗号鍵K P p yもしくは他のメモリカードのクラス鍵である公開暗号鍵K P m wによって暗号化してバスBS4に送出する暗号処理部1410と、バスBS4よりセッションキーK s 2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーK s 2によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵K cおよび再生制限A C pを、復号処理部1412で復号された移動セッションにおいて他のメモリカードに固有な公開暗号鍵K P m c x (x ≠ 8)で暗号化する暗号処理部1417とを含む。

【0092】メモリカード110は、さらに、バスBS4上のデータを公開暗号鍵K P m c 8と対をなすメモリカード110固有の秘密復号鍵K m c 8によって復号するための復号処理部1404と、逐次更新される証明書失効リストデータC R Lと、暗号化コンテンツデータ

{D c} K cと、暗号化コンテンツデータ{D c} K cを再生するためのライセンス(K c, A C p, A C m, ライセンスI D)と、付加情報D a t a - i n fとをバスBS4より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1515は、証明書失効リストC R Lを記録したC R L領域1415Aと、ライセンスを記録したライセンス領域1415Bと、暗号化コンテンツデータ{D c} K c、暗号化コンテンツデータの関連情報D c - i n fを記録したデータ領域1415Cとから成る。

50 【0093】また、C R L領域1415Aおよびライセ

ンス領域1415Bは、外部から直接アクセス不可能なセキュアなメモリ空間に設けられる。データ領域1415Cは外部からアクセス可能な通常のメモリ空間に設けられる。

【0094】メモ리카ード110は、さらに、バスBS4を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモ리카ード110の動作を制御するためのコントローラ1420を含む。

【0095】図7は、ポータブルステレオ120の構成を示す概略ブロック図である。ポータブルステレオ120は、ポータブルステレオを構成する各部とのデータの授受を行なうバスBS4と、携帯電話機100からの信号を受信するアンテナ2000と、アンテナ2000によって受信された信号をベースバンド信号に変換し、あるいはポータブルステレオからのデータを変調してアンテナ2000に与えるための送受信部2002と、メモ리카ード110に配信された暗号化コンテンツデータとライセンスとを携帯電話機100による通信によって受信し、その受信したライセンスによって暗号化コンテンツデータを再生するコンテンツ再生デバイス1550を含む。なお、コンテンツ再生デバイス1550は、図5に示すコンテンツ再生デバイスと同じ構成であるが、ポータブルステレオ120のコンテンツ再生デバイスにおいては、ポータブルステレオに固有なクラスyをy=1とする。したがって、認証データを{Kp p2/Cp p2} KPaから{Kp p1/Cp p1} KPaに代え、Kp保持部1502に保持する秘密復号鍵をKp保持部1502に代えている。その以外の部分については、図5に示したコンテンツ再生デバイスと同じである。

【0096】ポータブルステレオ120は、さらに、バスBS4を介してポータブルステレオ120の動作を制御するためのコントローラ2020と、外部からの指示をポータブルステレオ120に与えるための操作パネル2010と、コントローラ2020等から出力される情報をポータブルステレオのユーザに視覚情報として与えるための表示パネル2008を含む。

【0097】ポータブルステレオ120は、さらに、コンテンツ再生デバイス1550の音楽デコーダ1518からの音楽信号をLチャンネルのスピーカ用の音楽信号とRチャンネルのスピーカ用の音楽信号とに分離し、それぞれの音楽信号のノイズを除去するLPF2016、2018と、コントローラ2020からの指示信号をバスBS4から受けてデジタル信号からアナログ信号に変換するDA変換器2012と、DA変換器2012からのアナログ信号によって増幅率を制御するゲイン制御部2022を含む。

【0098】ポータブルステレオ120は、さらに、ゲイン制御部2022により制御された増幅率によってLPF2016、2018からのアナログ信号を、それぞ

れ、増幅する増幅器2024、2026と、増幅器2024からの信号を外部へ出力するスピーカ2028と、増幅器2026からの信号を外部へ出力するスピーカ2032を含む。

【0099】以降では、簡単化のためアクセス制限ACmは再生回数の制限を行なう制御情報である再生回数のみを、再生制限ACpは再生可能な期限を規定する制御情報である再生期限のみを制限するものとする。

【0100】以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0101】〔配信〕図1に示すデータ配信システムにおいて、配信サーバ10から携帯電話機100へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

【0102】図8～図11は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機100への配信動作（以下、配信セッションともいう）を説明するための第1～第4のフローチャートである。

【0103】図8における処理以前に、携帯電話機100のユーザは、配信サーバ10に携帯電話網を介して接続し、配信サーバ10のメニューデータベース307から提供されるメニューに従って配信（購入）を希望するコンテンツに対するコンテンツIDを取得していることを前提としている。

【0104】図8を参照して、携帯電話機100のユーザから操作パネル1108を介してコンテンツIDの指定による配信リクエストがなされる（ステップS100）。そして、操作パネル1108を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される（ステップS102）。つまり、選択した暗号化コンテンツデータを復号するライセンスを購入するために、暗号化コンテンツデータのアクセス制限ACm、および再生制限ACpを設定するための購入条件ACが入力される。

【0105】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1106は、バスBS2およびメモ리카ードインタフェース1200を介してメモ리카ード110へ認証データの出力指示を与える（ステップS104）。メモ리카ード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して認証データの出力指示を受取る。そして、コントローラ1420は、バスBS3を介して認証データ保持部1400から認証データ{Kp m7/Cm7} KPaを読み出し、{Kp m7/Cm7} KPaをバスBS3、インタフェース1424および端子1426を介して出力する（ステップS106）。

【0106】携帯電話機100のコントローラ1106は、メモ리카ード110からの認証データ{Kp m7/Cm7} KPaに加えて、コンテンツID、ライセン

ス購入条件AC、および配信リクエストを配信サーバ10に対して送信する(ステップS108)。

【0107】配信サーバ10では、携帯電話機100から配信リクエスト、コンテンツID、認証データ{K<sub>Pm7</sub>//C<sub>m7</sub>}K<sub>Pa</sub>、およびライセンス購入条件ACを受信し(ステップS110)、復号処理部312においてメモリカード110に出力された認証データを公開認証鍵K<sub>Pa</sub>で復号処理を実行する(ステップS112)。

【0108】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからの公開暗号鍵K<sub>Pm7</sub>と証明書C<sub>m7</sub>とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS114)。正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵K<sub>Pm7</sub>および証明書C<sub>m7</sub>を承認し、受理する。そして、次の処理(ステップS116)へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵K<sub>Pm7</sub>および証明書C<sub>m7</sub>を受理しないで処理を終了する(ステップS198)。

【0109】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、メモリカード110のクラス証明書C<sub>m7</sub>が証明書失効リストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が証明書失効リストの対象になっている場合には、ここで配信セッションを終了する(ステップS198)。

【0110】一方、メモリカード110のクラス証明書が証明書失効リストの対象外である場合には次の処理に移行する(ステップS116)。

【0111】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが証明書失効リストの対象外であることが確認されると、配信サーバ10において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する(ステップS118)。また、セッションキー発生部316は、配信のためのセッションキーK<sub>s1</sub>を生成する(ステップS120)。セッションキーK<sub>s1</sub>は、復号処理部312によって得られたメモリカード110に対応する公開暗号鍵K<sub>Pm7</sub>によって、暗号処理部318によって暗号化される(ステップS122)。

【0112】トランザクションIDおよび暗号化されたセッションキーK<sub>s1</sub>は、トランザクションID//{K<sub>s1</sub>}K<sub>m7</sub>として、バスBS1および通信装置350を介して外部に出力される(ステップS124)。

【0113】図9を参照して、携帯電話機100が、トランザクションID//{K<sub>s1</sub>}K<sub>m7</sub>を受信すると

(ステップS126)、コントローラ1106は、トランザクションID//{K<sub>s1</sub>}K<sub>m7</sub>をメモリカード110に入力する(ステップS128)。そうすると、メモリカード110においては、端子1426およびインタフェース1424を介して、バスBS3に与えられた受信データを、復号処理部1422が、保持部1421に保持されるメモリカード110に固有の秘密復号鍵K<sub>m7</sub>により復号処理することにより、セッションキーK<sub>s1</sub>を復号し、セッションキーK<sub>s1</sub>を受理する(ステップS130)。

【0114】コントローラ1420は、配信サーバ10で生成されたセッションキーK<sub>s1</sub>の受理を確認すると、セッションキー発生部1418に対してメモリカード110において配信動作時に生成されるセッションキーK<sub>s2</sub>の生成を指示する。そして、セッションキー発生部1418は、セッションキーK<sub>s2</sub>を生成する(ステップS132)。

【0115】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている証明書失効リストの更新日時CRLdateを抽出して切換スイッチ5246に出力する(ステップS134)。

【0116】暗号処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1422より与えられるセッションキーK<sub>s1</sub>によって、切換スイッチ1446の接点を順次切換えることによって与えられるセッションキーK<sub>s2</sub>、公開暗号鍵K<sub>Pmc8</sub>および更新日時CRLdateを1つのデータ列として暗号化して、{K<sub>s2</sub>//K<sub>Pmc8</sub>//CRLdate}K<sub>s1</sub>をバスBS3に出力する(ステップS136)。

【0117】バスBS3に出力された暗号化データ{K<sub>s2</sub>//K<sub>Pmc8</sub>//CRLdate}K<sub>s1</sub>は、バスBS3からインタフェース1424および端子1426を介して携帯電話機100に出力され、携帯電話機100から配信サーバ10に送信される(ステップS138)。

【0118】配信サーバ10は、トランザクションID//{K<sub>s2</sub>//K<sub>Pmc8</sub>//CRLdate}K<sub>s1</sub>を受信して、復号処理部320においてセッションキーK<sub>s1</sub>による復号処理を実行し、メモリカード110で生成されたセッションキーK<sub>s2</sub>、メモリカード110固有の公開暗号鍵K<sub>Pmc8</sub>およびメモリカード110における証明書失効リストの更新日時CRLdateを受理する(ステップS142)。

【0119】配信制御部315は、ステップS110で取得したコンテンツIDおよびライセンス購入条件ACに従って、アクセス制限AC<sub>m</sub>および再生制限AC<sub>p</sub>を生成する(ステップS144)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵K<sub>c</sub>を情報データベース304より取得する(ステップS146)。

10

20

30

40

50

【0120】配信制御部315は、生成したライセンス、すなわち、トランザクションID、コンテンツID、ライセンス鍵Kc、再生制限ACp、およびアクセス制限ACmを暗号処理部326に与える。暗号処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kp<sub>mc8</sub>によってライセンスを暗号化して暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>を生成する(ステップS148)。

【0121】図10を参照して、配信サーバ10において、メモリカード110から送信された証明書失効リストの更新日時CRLdateが、CRLデータベース306に保持される配信サーバ10における失効証明書リストCRLの更新日時と比較することで最新か否かが判断され、データCRLdateが最新と判断されたとき、ステップS152へ移行する。また、データCRLdateが最新でないときはステップS160へ移行する(ステップS150)。

【0122】データCRLdateが最新と判断されたとき、暗号処理部328は、暗号処理部326から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>をメモリカード110において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>}Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>}Ks2を通信装置350を介して携帯電話機100へ送信する(ステップS152)。

【0123】そして、携帯電話機100のコントローラ1106は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>}Ks2を受信し(ステップS154)、バスBS5を介してメモリカード110に入力する。メモリカード110の復号処理部1412は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>}Ks2を端子1426およびインタフェース1424を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>を受理する(ステップS158)。その後、ステップS172へ移行する。

【0124】一方、配信サーバ10において、CRLdateが最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の証明書失効リストのデータCRLdateを取得し、差分データである差分CRLを生成する(ステップ

S160)。

【0125】暗号処理部328は、暗号処理部326の出力と、配信制御部315がバスBS1を介して供給する証明書失効リストの差分CRLとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号処理部328より出力された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>}Ks2は、バスBS1および通信装置350を介して携帯電話機100に送信される(ステップS162)。

【0126】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0127】携帯電話機100は、送信された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>}Ks2を受信し(ステップS164)、バスBS2を介してメモリカード110に入力する(ステップS166)。メモリカード110においては、端子1426およびインタフェース1424を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3の受信データを復号しバスBS3に出力する(ステップS168)。

【0128】この段階で、バスBS3には、K<sub>mc</sub>保持部5221に保持される秘密復号鍵K<sub>mc8</sub>で復号可能な暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}K<sub>mc8</sub>と、差分CRLとが出力される(ステップS168)。コントローラ1420の指示によって受理した差分CRLによってメモリ1415内のCRL領域1415Aを差分CRLに基づいて更新する(ステップS170)。

【0129】ステップS152、S154、S156、S158は、メモリカード110が保持する証明書失効リストCRLdateが最新の場合のメモリカード110へのライセンスの配信動作であり、ステップS160、S162、S164、S166、S168、S170は、メモリカード110が保持する証明書失効リストCRLが最新でない場合のメモリカード110へのライセンスの配信動作である。このように、メモリカード110から送られてきた証明書失効リストCRLdateが最新か否かを、逐一、確認し、最新でないとき、最新の証明書失効リストCRLをCRLデータベース306から取得し、差分CRLをメモリカード110に配信す

10

20

30

40

50

ることによって、配信したライセンスが、秘密復号鍵が漏洩したり、TRMが破られた不正なメモリカードやコンテンツ再生デバイスへ出力されることを防止できる。

【0130】ステップS158またはステップS170の後、コントローラ1420の指示によって、暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8は、復号処理部1404において、秘密復号鍵Kmc8によって復号され、ライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限ACmおよび再生制限ACp)が受理される(ステップS172)。

【0131】図11を参照して、コントローラ1420は、受理したライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制限ACmおよび再生制限ACp)をメモリ1415のライセンス領域1415Bに記録する(ステップS174)。

【0132】携帯電話機100のコントローラ1106は、配信サーバ10から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ10へ送信する(ステップS178)。

【0133】配信サーバ10は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し(ステップS180)、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する(ステップS182)。

【0134】携帯電話機100は、{Dc}Kc//Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受理する(ステップS184)。そして、コントローラ1106は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infをバスBS2およびメモリカードインタフェース1200を介してメモリカード110へ出力する。そうすると、メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS3を介して暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受取り、バスBS3を介して暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infをメモリ1415のデータ領域1515Cに記録する(ステップS190)。そして、携帯電話機100のコントローラ1106は、トランザクションIDと配信受理を配信サーバ10へ送信する(ステップS192)。

【0135】配信サーバ10は、トランザクションID//配信受理を受信すると(ステップS194)、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行われて配信終了の処理が実行され(ステップS196)、全体の処理が終了する(ステップS198)。

【0136】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm7とともに暗号化して送信できた公開暗号鍵Kpm7が有効であることを確認した上で、クラス証明書Cm7が証明書失効リスト、すなわち、公開暗号鍵Kpm7による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0137】[再生]次に、図12および図13を参照してメモリカード110に記録されたコンテンツデータのポータブルステレオ120(コンテンツ再生デバイスとも言う、以下同じ)における再生動作について説明する。図12を参照して、再生動作の開始とともに、ポータブルステレオ120のユーザから操作パネル2010を介して再生指示がポータブルステレオ120にインプットされる(ステップS1000)。そうすると、コントローラ2020は、バスBS4を介して認証データ保持部1500から認証データ{Kpp1//Cp1}KPaを読み出し、送受信部2002を介して携帯電話機100へ認証データ{Kpp1//Cp1}KPaを出力する(ステップS1002)。

【0138】そうすると、携帯電話機100においてコントローラ1106は、アンテナ1103および送受信部1104を介して認証データ{Kpp1//Cp1}KPaを受信し、メモリカードインタフェース1200を介して認証データ{Kpp1//Cp1}KPaをメモリカード110へ出力する。そして、メモリカード110は、認証データ{Kpp1//Cp1}KPaを受理する(ステップS1004)。そして、メモリカード110の復号処理部1408は、受理した認証データ{Kpp1//Cp1}KPaを、KPa保持部1414に保持された公開認証鍵KPaによって復号し(ステップS1006)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kpp1//Cp1}KPaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS1008)。復号できなかった場合、ステップS1048へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、取得した証明書Cp1がメモリ1415から読出した証明書失効リストデータCRLに含まれるか否かを判断する(ステップS1010)。この場合、証明書Cp1にはIDが付与されており、コントローラ1420は、受理した証明書Cp1のIDが証明書失効リストデータの中に存在するか否かを判別する。証明書Cp1が証明書失効リストデータに含まれると判断されると、ステップS1048へ移行し、再生動作は終了する。

【0139】ステップS1010において、証明書Cp

1が証明書失効リストデータCRLに含まれていないと判断されると、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS1012)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した{Ks2}Kp1をバスBS3へ出力する(ステップS1014)。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ{Ks2}Kp1を出力する(ステップS1016)。携帯電話機100のコントローラ1106は、メモリカードインタフェース1200を介して{Ks2}Kp1を取得し、その取得した暗号化データ{Ks2}Kp1を送受信部1104を介してポータブルステレオ120へ送信する。そうすると、ポータブルステレオ120のコントローラ2020は、アンテナ2000および送受信部2002を介して暗号化データ{Ks2}Kp1を受信し、復号処理部1504へ暗号化データ{Ks2}Kp1を与える。そして、Kp保持部1502は、秘密復号鍵Kp1を復号処理部1504へ出力する。

【0140】復号処理部1504は、Kp1保持部1502から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号処理部1506へ出力する(ステップS1018)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1506へ出力する(ステップS1020)。暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を復号処理部1504からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し、コントローラ2020は、バスBS4および送受信部2002を介して暗号化データ{Ks3}Ks2を携帯電話機100へ送信する(ステップS1022)。

【0141】そうすると、携帯電話機100のコントローラ1106は、送受信部1104を介して暗号化データ{Ks3}Ks2を受信し、メモリカードインタフェース1200を介して暗号化データ{Ks3}Ks2をメモリカード110へ出力する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して暗号化データ{Ks3}Ks2を受信し、復号処理部1412へ与える(ステップS1024)。

【0142】図13を参照して、復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、ポータブルステレオ120のコンテンツ再生デバ

イス1550で発生されたセッションキーKs3を受理する(ステップS1026)。セッションキーKs3の受理に応じて、コントローラ1420は、アクセス制限ACmを確認する(ステップS1028)。ステップS1028においては、メモリのアクセスに対する制限に関する情報であるアクセス制限ACmを確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限に制限がある場合にはアクセス制限ACmのデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS1030)。一方、アクセス制限ACmによって再生回数が制限されていない場合においては、ステップS1030はスキップされ、アクセス制限ACmは更新されることなく処理が次のステップ(ステップS1032)に進行される。

【0143】ステップS1028において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Bに記録された再生リクエスト曲のライセンス鍵Kcおよび再生制限ACpがバスBS4上に出力される(ステップS1032)。

【0144】得られたライセンス鍵Kcと再生制限ACpは、切換スイッチ1446の接点Pfを介して暗号処理部1406に送られる。暗号処理部1406は、切換スイッチ1442の接点Pbを介して復号処理部1412より受けたセッションキーKs3によって切換スイッチ1446を介して受けたライセンス鍵Kcと再生制限ACpとを暗号化し、{Kc//ACp}Ks3をバスBS3に出力する(ステップS1034)。

【0145】バスBS3に出力された暗号化データ{Kc//ACp}Ks3は、インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して携帯電話機100に送出される。

【0146】携帯電話機100のコントローラ1106は、暗号化データ{Kc//ACp}Ks3を受取り、送受信部1104を介して暗号化データ{Kc//ACp}Ks3をポータブルステレオ120へ送信する。そして、ポータブルステレオ120のコントローラ2020は、送受信部2002を介して暗号化データ{Kc//ACp}Ks3を受信し、その受信した暗号化データ{Kc//ACp}Ks3を復号処理部1510に与える。復号処理部1510は、暗号化データ{Kc//ACp}Ks3をセッションキーKs3によって復号し、ライセンス鍵Kcおよび再生制限ACpを受理する(ステップS1036)。復号処理部1510は、ライセンス鍵Kcを復号処理部1516に伝達し、再生制限ACpをバスBS4に出力する。

【0147】コントローラ2020は、バスBS4を介して、再生制限ACpを受理して再生の可否の確認を行なう(ステップS1040)。

【0148】ステップS1040においては、再生制限

ACpによって再生不可と判断される場合には、再生動作は終了される。

【0149】ステップS1040において再生可能と判断された場合、コントローラ2020は、送受信部2002、携帯電話機100を介してメモ리카ード110に暗号化コンテンツデータ{Dc}Kcを要求する。そうすると、メモ리카ード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Dc}Kcを取得し、バスBS3、インタフェース1424、および端子1426を介してメモ리카ードインタフェース1200へ出力する(ステップS1042)。

【0150】携帯電話機100のコントローラ1106は、メモ리카ードインタフェース1200を介して暗号化コンテンツデータ{Dc}Kcを取得し、送受信部1104を介して暗号化コンテンツデータ{Dc}Kcをポータブルステレオ120へ送信する。ポータブルステレオ120のコントローラ2020は、送受信部2002を介して暗号化コンテンツデータ{Dc}Kcを受信し、バスBS4を介して暗号化コンテンツデータ{Dc}Kcを復号処理部1516へ与える。

【0151】そして、復号処理部1516は、暗号化コンテンツデータ{Dc}Kcを復号処理部1510から出力されたライセンス鍵Kcによって復号してコンテンツデータDcを取得する(ステップS1044)。

【0152】そして、復号されたコンテンツデータDcは音楽デコーダ1518へ出力され、音楽デコーダ1518は、コンテンツデータを再生し、再生したアナログ信号である音楽信号をLチャンネルスピーカ用の信号とRチャンネルスピーカ用の信号とに分離してLPF2016、2018へ出力する。そして、音楽信号はLPF2016、2018でノイズを除去され、増幅器2024、2026でゲイン制御部2022によって制御された増幅率に増幅され、スピーカ2028、2030から外部へ出力されて再生される(ステップS1046)。これによって再生動作が終了する。

【0153】上記においては、携帯電話機100に装着されたメモ리카ード110に記録された暗号化コンテンツデータをポータブルステレオによって再生する場合について説明したが、ポータブルステレオ120にメモ리카ード110が装着された場合も、上述したフローチャートに従って暗号化コンテンツデータが再生される。

【0154】また、上述したように携帯電話機100は、コンテンツ再生デバイス1550を内蔵するので、携帯電話機100はメモ리카ード110に記録された暗号化コンテンツデータを上述したフローチャートに従って再生することが可能である。

【0155】本発明によるポータブルステレオは、図7に示すものに限らず、図14に示すポータブルステレオ120Aであっても良い。ポータブルステレオ120Aは、本体121と、スピーカ2028、2032とから

成り、携帯電話機100Aの充電台が設けられた携帯電話機充電台兼用型のポータブルステレオである。

【0156】図15は、ポータブルステレオ120Aのブロック図を示したものである。ポータブルステレオ120Aは、図7に示すポータブルステレオ120に充電部2500を追加したものであり、それ以外はポータブルステレオ120と同じである。充電部2500は、電源2501と、電圧制御部2502と、誘導コイル2503とから成る。電圧制御部2502は電源2501から供給される電力に基づいて誘導コイル2503によって発生される電圧を制御する。誘導コイル2503は、電圧制御部2502によって制御された電圧を伝える、誘導磁界を発生させ、携帯電話機100Aを充電する。

【0157】図16は、ポータブルステレオ120Aに設置される携帯電話機100Aの構成を示すブロック図である。携帯電話機100Aは、図5に示す携帯電話機100に充電部1130を追加したものであり、その他は携帯電話機100と同じである。充電部1130は、誘導コイル1132と、電流制御部1134と、電池1136とから成る。誘導コイル1132は、ポータブルステレオ120の誘導コイル2503によって発生した誘導磁界に反応して、誘導電流を発生する。この時の電圧は、ポータブルステレオ120の電圧制御部2502によって制御される。誘導コイル1132は、電流制御部1134に誘導電流を供給し、電流制御部1134は、電池へ供給する電流を制御し、電池へ充電用電流を提供する。そして、電池1134は、電流制御部1134からの電流によって充電される。

【0158】図16に示す携帯電話機100Aは、図8～図11に示すフローチャートに従って配信サーバ10から暗号化コンテンツデータおよびライセンスを受信してメモ리카ードインタフェース1200を介してメモ리카ード110に暗号化コンテンツデータおよびライセンスを記録する。そして、図15に示すポータブルステレオ120Aは、図12、13に示すフローチャートに従って携帯電話機100Aから暗号化コンテンツデータおよびライセンスを受信して再生する。

【0159】このように、携帯電話機と一体型になったポータブルステレオにおいては、携帯電話機を設置したままで、暗号化コンテンツデータおよびライセンスを配信サーバから受信できるとともに、メモ리카ードに記録された暗号化コンテンツデータをスムーズに再生できる。

【0160】本発明におけるポータブルステレオは、図17に示すポータブルステレオ120Bであっても良い。ポータブルステレオ120Bは、ハンドフリーの機能付きポータブルステレオであり、図7に示すポータブルステレオ120に音声入力部124を追加したものである。そして、ポータブルステレオ120Bと通信する携帯電話機は、ポータブルステレオが音声入力部124

に対応した構成を有する携帯電話機100Bである。その他は、図7に示すポータブルステレオ120と同じである。

【0161】図18は、ポータブルステレオ120Bのブロック図を示したものである。ポータブルステレオ120Bは、図7に示すポータブルステレオ120に音声入力部124と、音声コーデック2034と、DA変換器2014と、混合器2036とを追加したものであり、それ以外は図7に示すポータブルステレオ120と同じである。

【0162】音声入力部124は、マイク1241と、増幅器1242と、バンドパスフィルタ(BPF)1243と、AD変換機1244とから成る。マイク1241から入力された音声は増幅器1242で増幅され、BPF1243でノイズを除去される。そして、音声は、マイク1241から入力されて、電気信号である音声信号としてAD変換機1244に入力され、アナログ信号からデジタル信号に変換されて音声コーデック2034に入力される。

【0163】そうすると、音声コーデック2034は、送話信号を所定の方式に符号化した送話データとして送受信部2002へ出力する。そして、送受信部2002は、入力した送話データを携帯電話器100Bへ送信する。また、携帯電話機から送信され、かつ、符号化された受話音声データは音声コーデック2034に入力され、受話音声データとして復号され、DA変換器2014にてデジタル信号からアナログ信号へ変換され、音声信号として混合器2036へ供給される。混合器2036は音声信号と、音楽デコーダ1518の出力である音楽信号を、コントローラ2020の指示に従って、選択的あるいは混合して2つのLPF2016、2018へ出力するものである。

【0164】つまり、ポータブルステレオ120Bは、音声入力部124からユーザの音声を入力し、その音声を携帯電話機100Bを介して外部と通話する機能を有するポータブルステレオであり、自動車に搭載されるカーステレオとしてハンズフリー通話機能を付加したものである。同様に、ポータブルステレオ120および120Aについてもカーステレオとして用いることが可能である。

【0165】図19は、図18に示すポータブルステレオ120Bからの音声信号を受け、その受けた音声信号を外部へ送信する機能を有する携帯電話機である。したがって、携帯電話機100Bは、外部へ音声を送受信するアンテナ1101および送受信部1102と、ポータブルステレオ120Bとの信号を送受信するアンテナ1103および送受信部1104とを有する。

【0166】図19に示す携帯電話機100Bは、図8～図11に示すフローチャートに従って配信サーバ10から暗号化コンテンツデータおよびライセンスを受信し

てメモ리카ードインタフェース1200を介してメモ리카ード110に暗号化コンテンツデータおよびライセンスを記録する。そして、図18に示すポータブルステレオ120Bは、図12、13に示すフローチャートに従って携帯電話機100Bから暗号化コンテンツデータおよびライセンスを受信して再生するとともに携帯電話機100Bを介して外部と通話する。

【0167】本発明においては、ポータブルステレオ120および120Aは、配信を受ける機能を備える携帯電話機100および100Aに変えて、再生専用機を用いることも可能である。その場合、再生専用機は、携帯電話機100および100Aを備える、携帯電話網を介した通話および配信の受信に用いる通信機能を省いた構成となる。

【0168】携帯電話器100Aに対応する再生専用機100Cは、図20に示すようにアンテナ1103と、送受信部1104と、充電部1130と、コンテンツ再生デバイス1550と、コントローラ1106と、表示パネル1108と、操作パネル1110と、メモ리카ードインタフェース1200とを備える。

【0169】同様に、図示しないが、携帯電話機100に対応する再生専用機は、図20の再生専用機100Cにおける充電部1130を省いた構成となる。

【0170】なお、上述したポータブルステレオ120、120A、および120Bは、携帯電話機または再生専用機からの暗号化コンテンツデータを再生する他、メモ리카ードインタフェース2030にメモ리카ード110を装着することで、直接メモ리카ードからライセンス鍵と暗号化コンテンツデータを取得して、音楽を再生することが可能である。この場合、送受信部2002を介して行なうデータの授受を、メモ리카ードインタフェース2030を介して、直接メモ리카ード110との間で行うようにすればよく、再生動作は図12および図13のフローチャートに従う。

【0171】また、ポータブルステレオ120、120Aおよび120BはCD、カセットテープ、MD等の再生機能を備えた構成として、CD、カセットテープ、MD等に記録された平文の音楽データも再生するものとしてもよい。

【0172】さらに、ポータブルステレオ120、120Aおよび120Bはメモ리카ードインタフェース2030を備えない構成としても良い。

【0173】また、上記においては、メモ리카ード110は、携帯電話機100を用いて配信サーバ10から暗号化コンテンツデータおよびライセンスを受信するとして説明したが、本発明においては、メモ리카ード110は音楽データが記録された音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得しても良い。一般には、メモ리카ード110は、どんな方法によって暗号化コンテンツデータおよびライセンスを



取得しても良い。したがって、本発明は、暗号化コンテンツデータおよびライセンスを記録したメモリカードから通信によって暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータを再生するポータブルステレオに適用される。

【0174】本発明の実施の形態によれば、ポータブルステレオは、暗号化コンテンツデータおよびライセンスを記録したメモリカードが装着された携帯電話機から暗号化コンテンツデータおよびライセンスを受信して再生するので、通信機能を有しないカーステレオまたはコン

ポーネントステレオであっても、暗号化コンテンツデータを再生できる。

【0175】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

#### 【図面の簡単な説明】

【図1】 本発明の実施の形態におけるデータ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図5】 図1に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図6】 図1に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図7】 図1に示すデータ配信システムにおけるポータブルステレオの構成を示す概略ブロック図である。

【図8】 図1に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第1のフローチャートである。

【図9】 図1に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第2のフローチャートである。

【図10】 図1に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第3のフローチャートである。

【図11】 図1に示すデータ配信システムにおける携帯電話機への配信動作を説明するための第4のフローチャートである。

【図12】 図1に示すデータ配信システムにおける携帯電話機における再生動作を説明するための第1のフローチャートである。

【図13】 図1に示すデータ配信システムにおける携帯電話機における再生動作を説明するための第2のフロ

ーチャートである。

【図14】 図1に示すデータ配信システムにおけるポータブルステレオの他の構成図である。

【図15】 図1に示すデータ配信システムにおけるポータブルステレオの他の概略ブロック図である。

【図16】 図1に示すデータ配信システムにおける携帯電話機の他の概略ブロック図である。

【図17】 図1に示すデータ配信システムにおけるポータブルステレオのさらに他の構成図である。

10 【図18】 図1に示すデータ配信システムにおけるポータブルステレオのまたさらに他の概略ブロック図である。

【図19】 図1に示すデータ配信システムにおける携帯電話機のさらに他の概略ブロック図である。

【図20】 再生専用機の構成を示す概略ブロック図である。

#### 【符号の説明】

10 配信サーバ、20 無線基地局、100, 100A, 100B 携帯電話機、110 メモリカード、120, 120A, 120B ポータブルステレオ、100C 再生専用機、121 本体、124 音声入力部、130 ヘッドホン、302 課金データベース、304 情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312, 320, 1404, 1408, 1412, 1422, 1504, 1510, 1516 復号処理部、313 認証鍵保持部、315 配信制御部、316, 1418 セッションキー発生部、318, 326, 328, 1406, 1410, 1417, 1506 暗号処理部、350 通信装置、1106, 1420, 2020 コントローラ、1101, 1103, 2000 アンテナ、1102, 1104, 2002 送受信部、1114, 1120, 1124, 1426 端子、1108, 2010 操作パネル、1110, 2008 表示パネル、1112 音声処理部、1114, 1241マイク、1116, 2028, 2032 スピーカ、1118, 2036 混合器、1122 外部インタフェース、1126, 1128, 2034 音声コーデック、1134 電流制御部、1136 電池、1200, 2030 メモリカードインタフェース、1243 BPF、1244 AD変換器、1400, 1500 認証データ保持部、1402 Kmc保持部、1414 KPa保持部、1415 メモリ、1415A CRL領域、1415B ライセンス領域、1415C データ領域、1416 KPmc保持部、1421 Km保持部、1424 インタフェース、1442, 1446 切換スイッチ、1502 Kp保持部、1518 音楽デコーダ、2012, 2014 DA変換器、1550 コンテンツ再生デバイス、2016, 2018 LPF、2

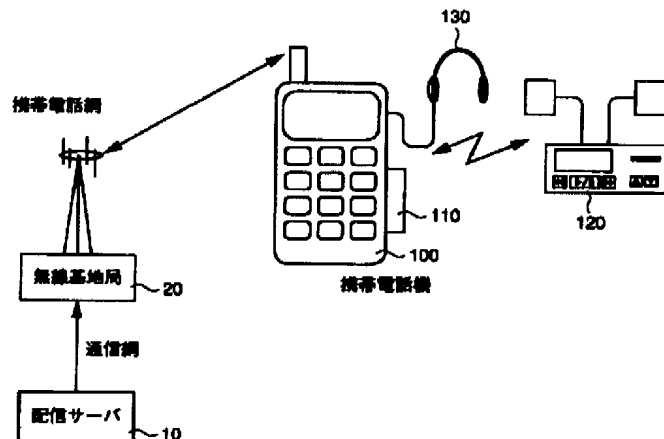
33

34

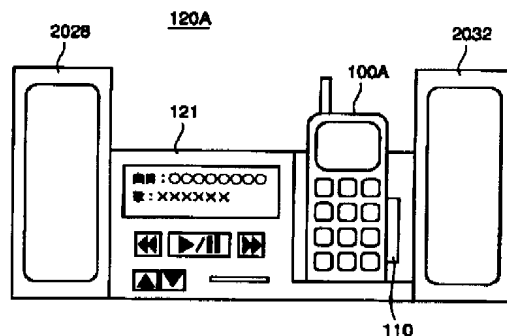
022ゲイン制御部、1242、2024、2026  
増幅器、1130、2500充電部、2501 電源、

2502 電圧制御部、1132, 2503 誘導コイル。

【图 1】



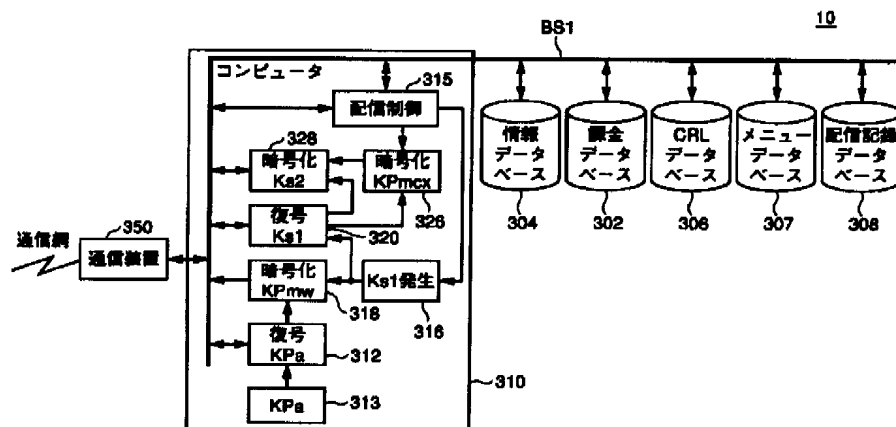
【图 14】



【图 2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ [Dc]Kcとして配信され、メモ리카ードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付属する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス鍵 暗号化コンテンツデータを復号する復号鍵
ACmVACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	ライセンス固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID+コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc+ACm+VACp+ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止認証データのリスト CRLの更新日(CRLdate)を含む

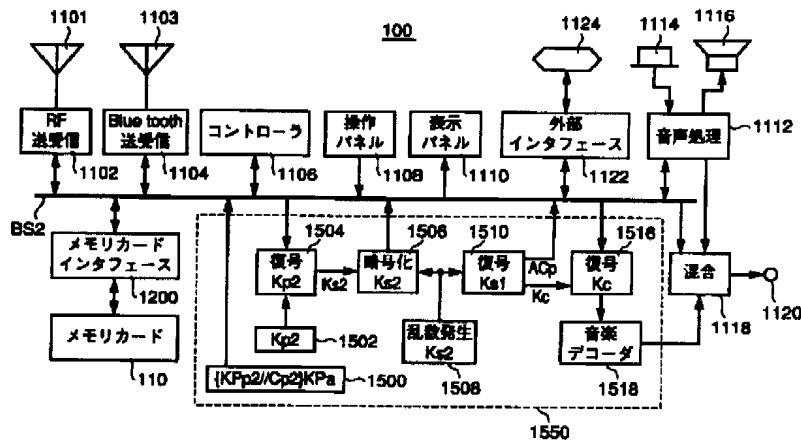
【図 4】



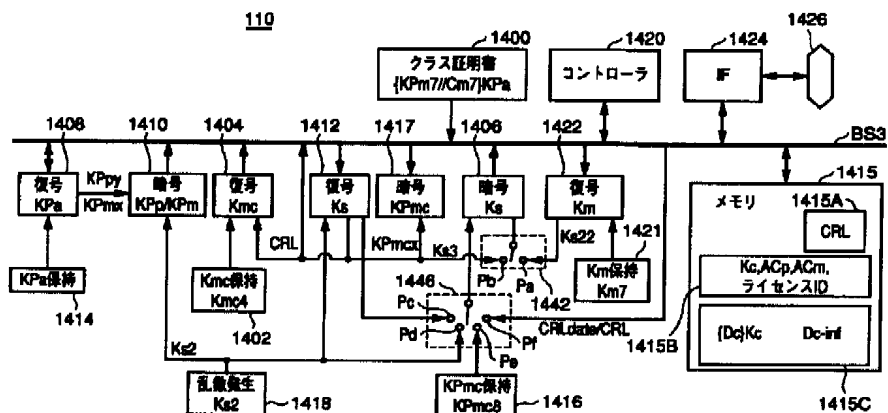
【図 3】

	記号	種類	属性	特性
配信サーバ	KPa	公開鍵暗号	システム共通	認証局にて認証された認証データを復号する鍵 メモリカードおよびコンテンツ管理モジュールと同一
	Ks1	共通鍵	セッション固有	メモリカードへのライセンスの配信時に発生
メモリカード	KPa	公開鍵暗号	システム共通	認証局にて認証された認証データを復号する鍵 配信サーバと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受時に発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。認証機能を有する。 {KPmw/Cmw}KPaの形式で出荷時に記録。 ※メモリカードのクラスwごとに異なる。
コンテンツ 再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cpyとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッション時に発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy/Cpy}KPaの形式で出荷時に記録。 ※コンテンツ再生デバイスのクラスyごとに異なる。

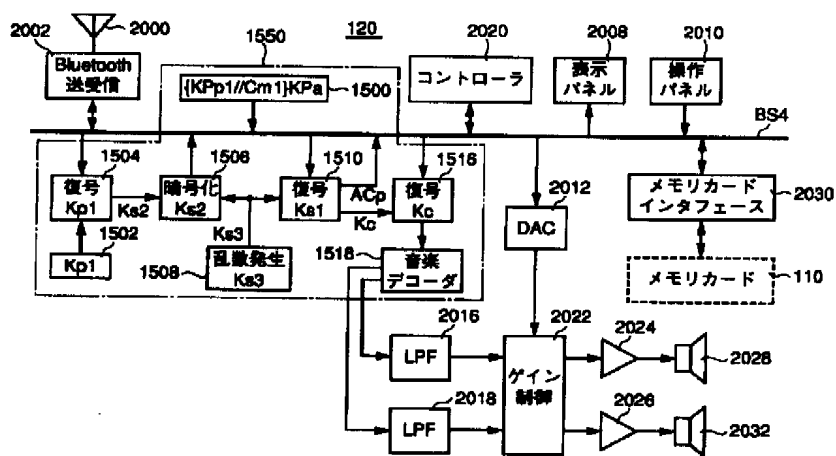
【図 5】



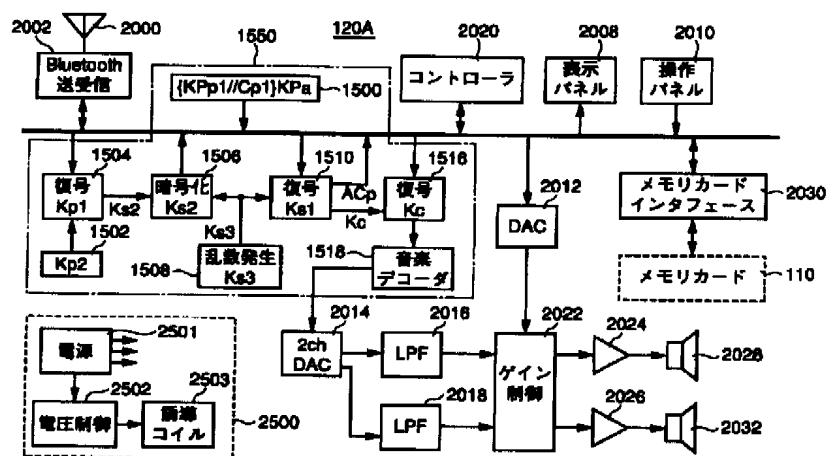
【図 6】



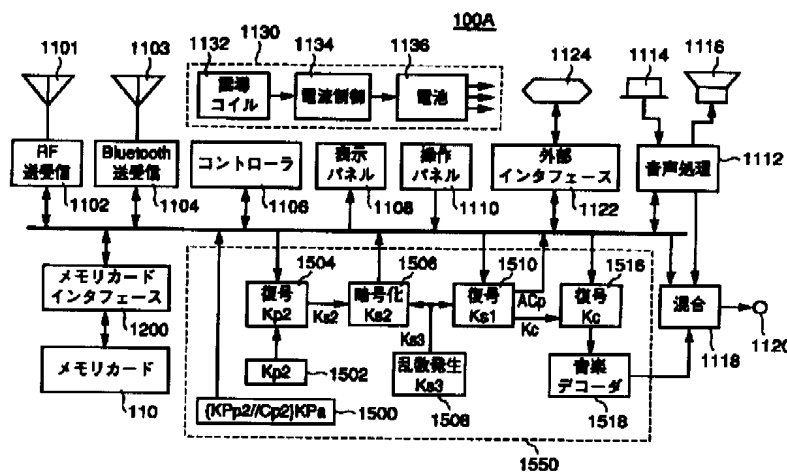
【図 7】



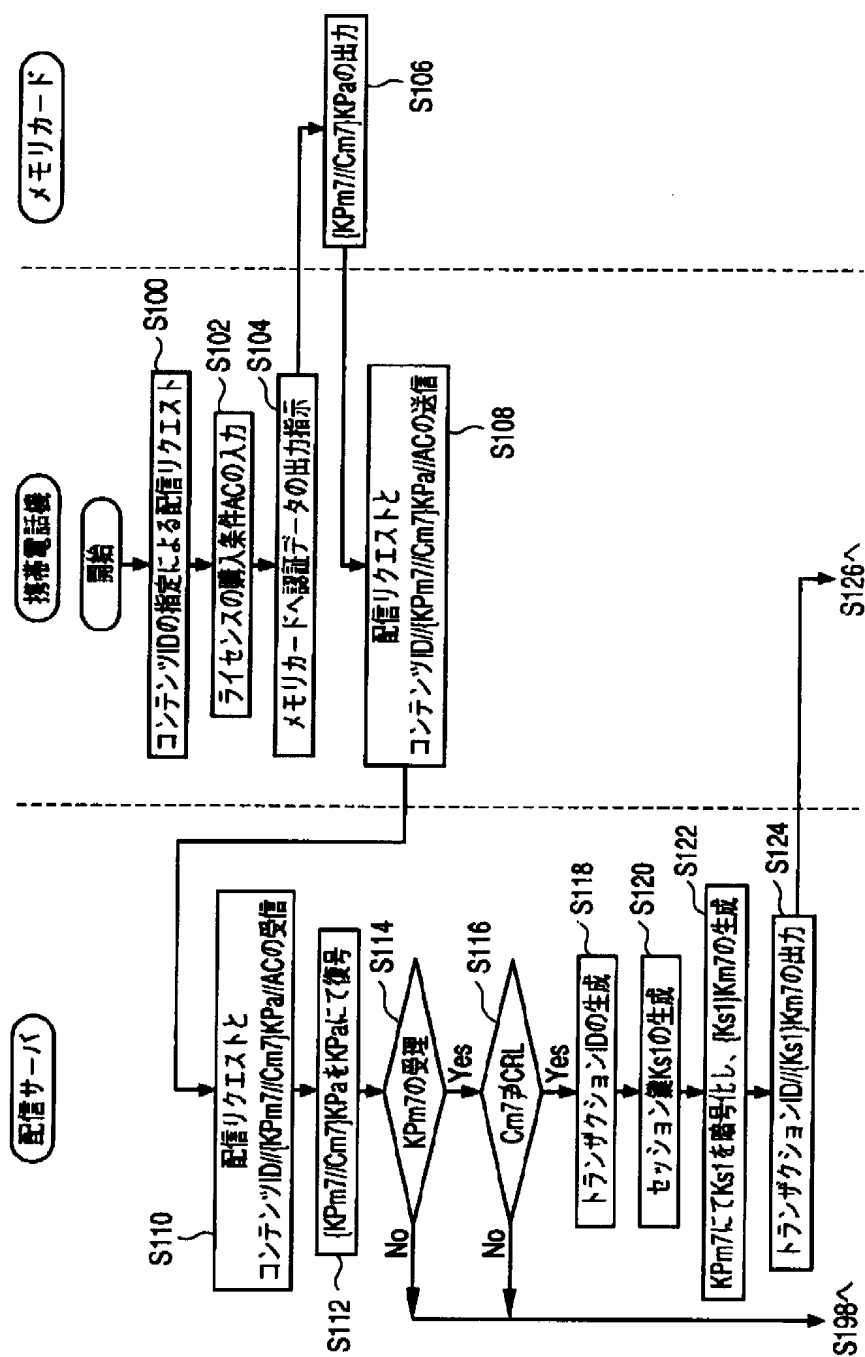
【図 15】



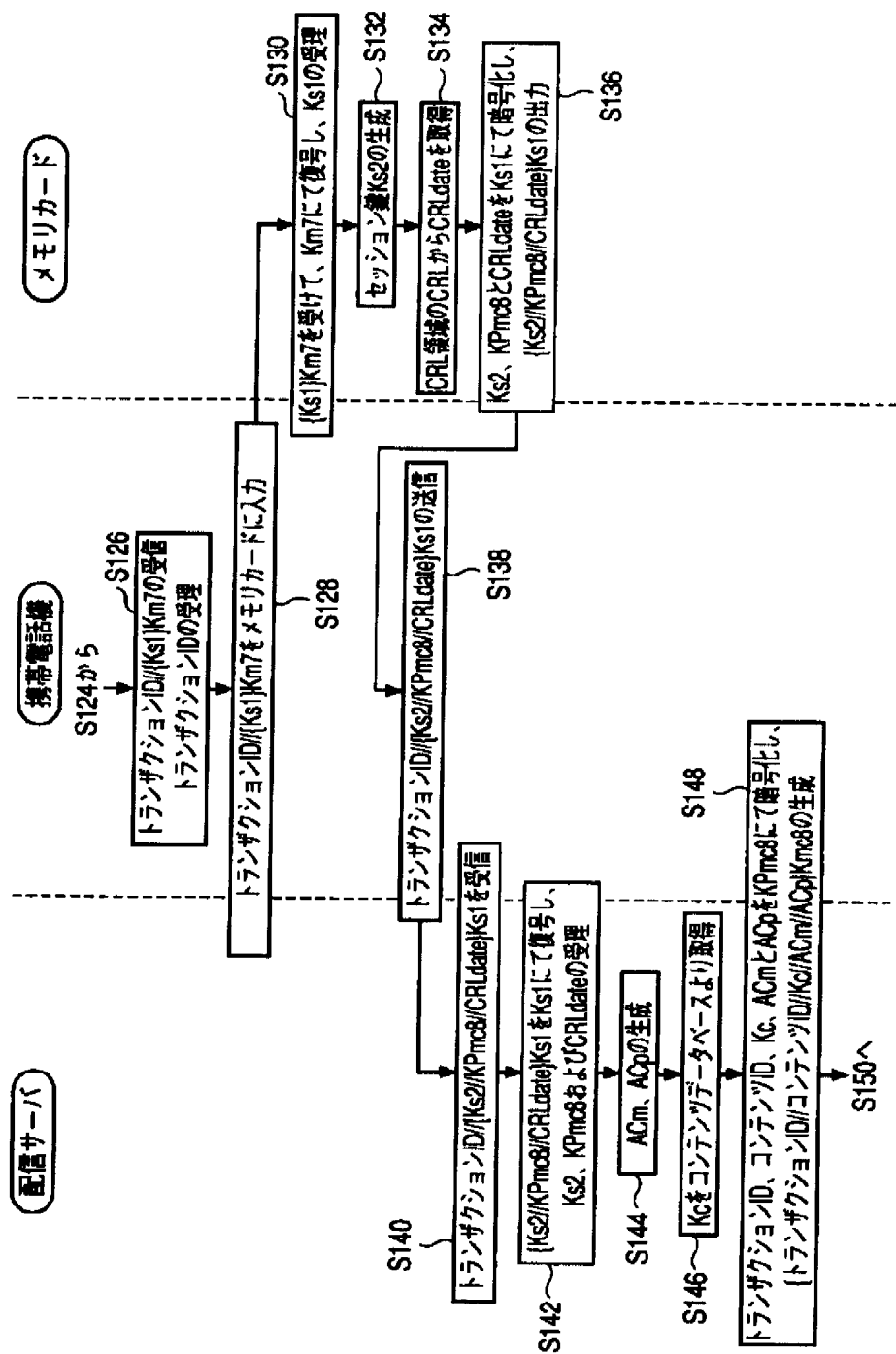
【図 16】



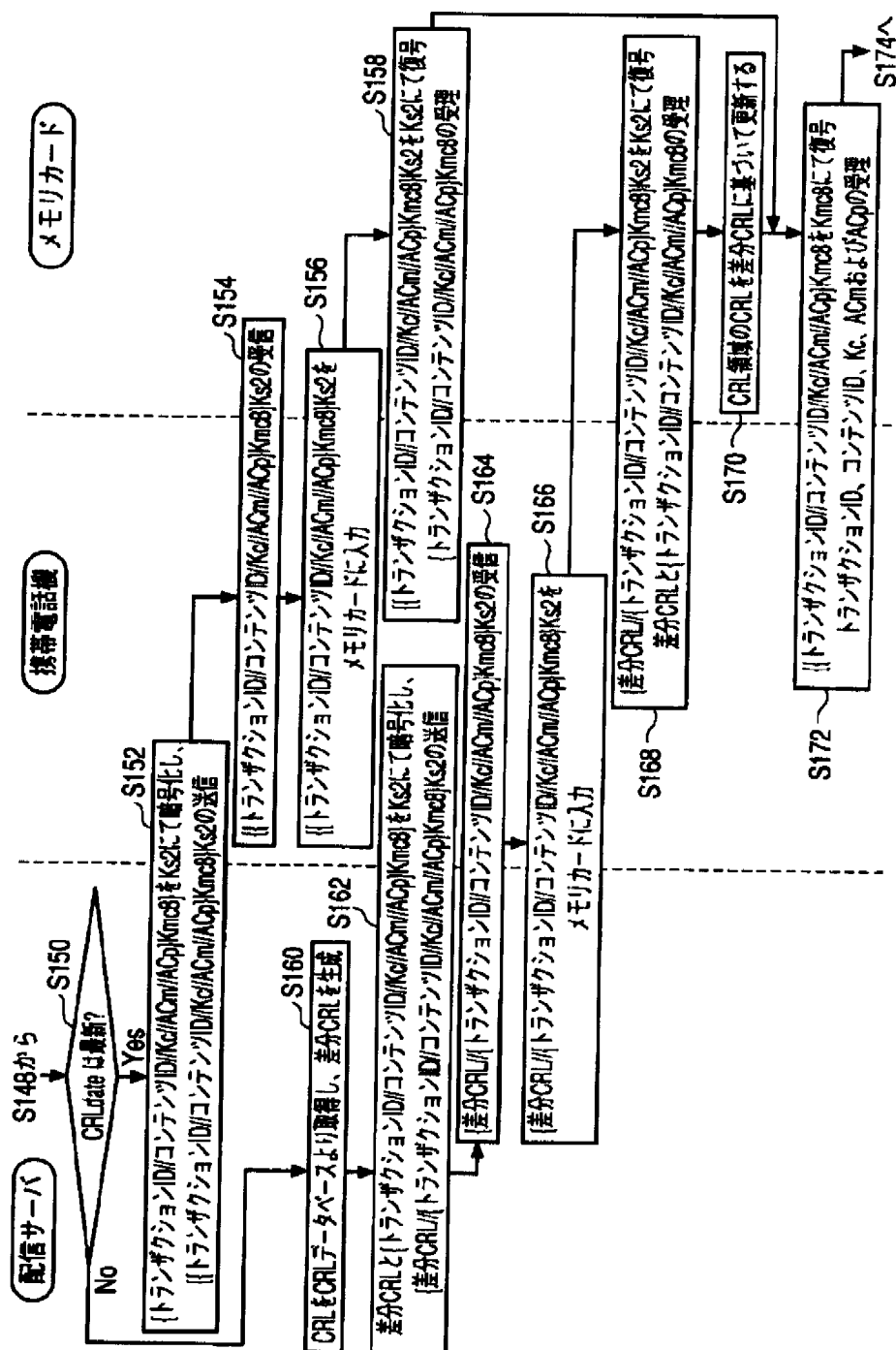
【図8】



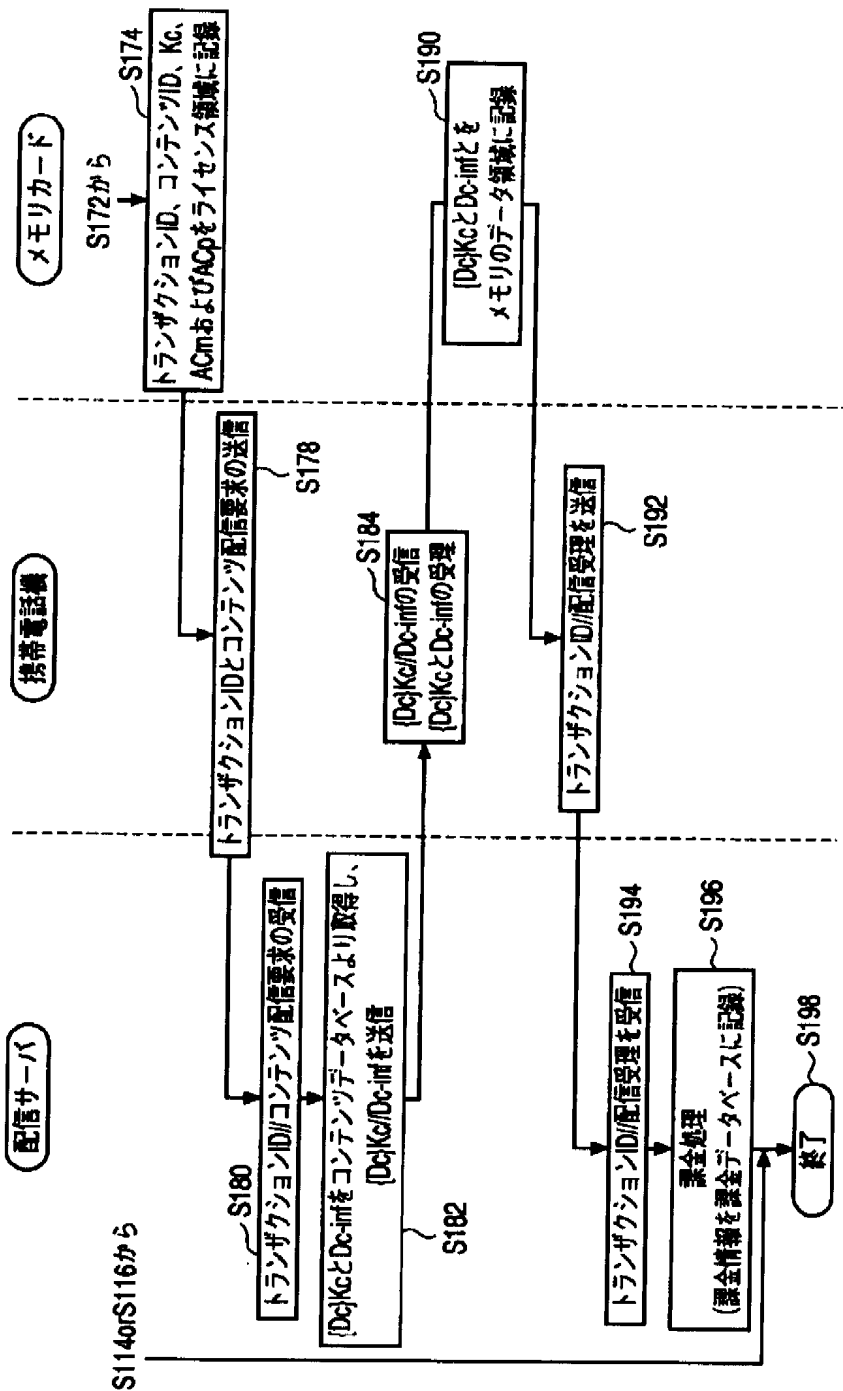
【図9】



【図10】

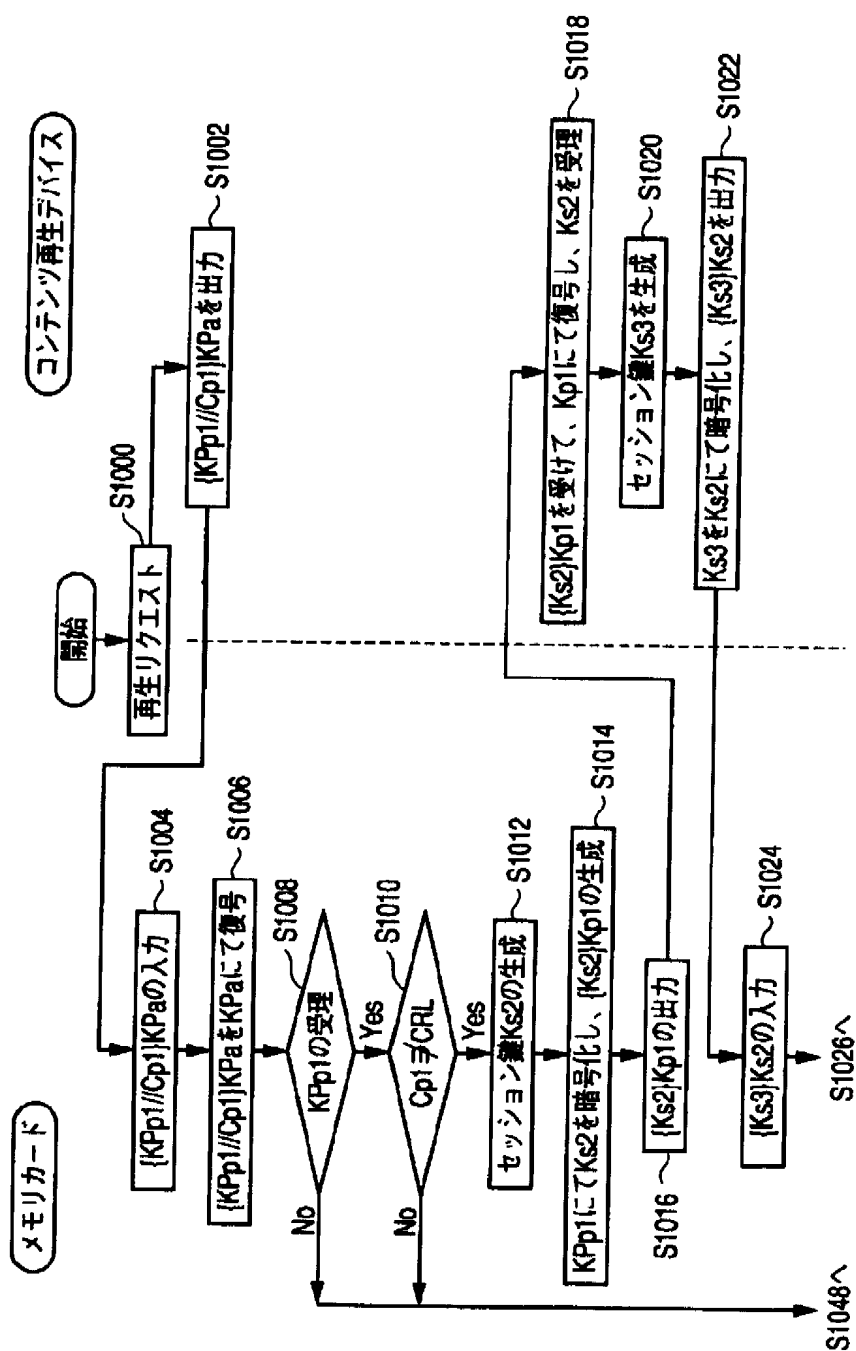


【図11】

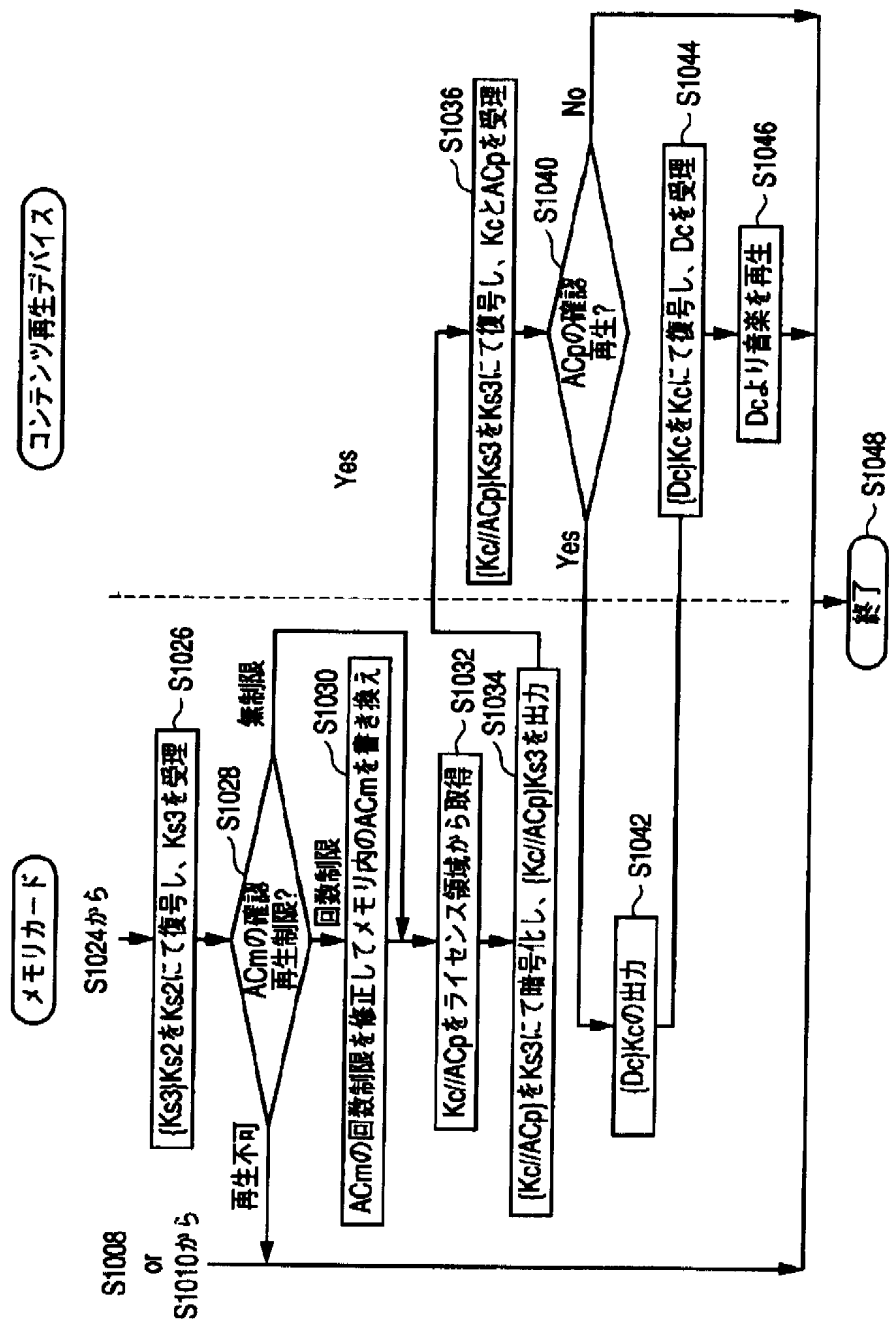




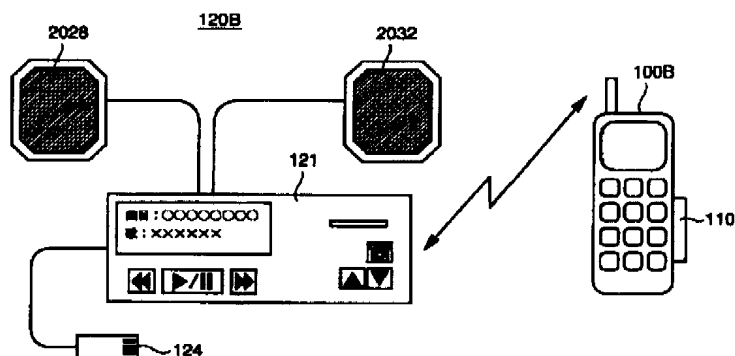
【図12】



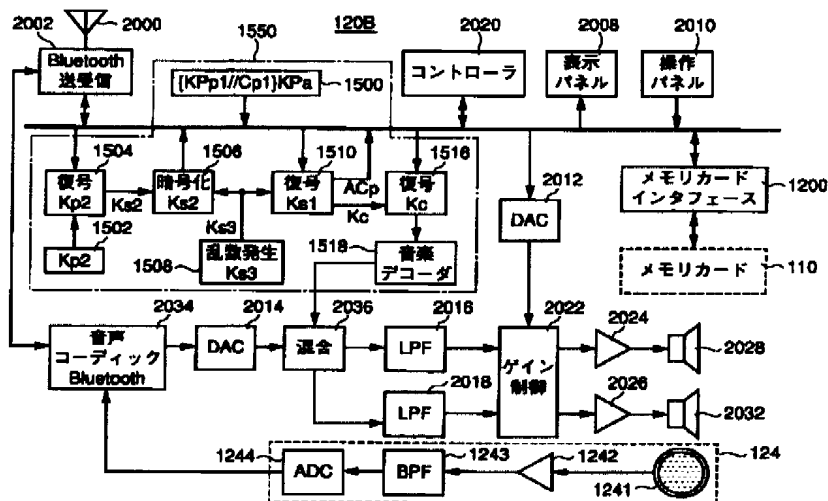
【図13】



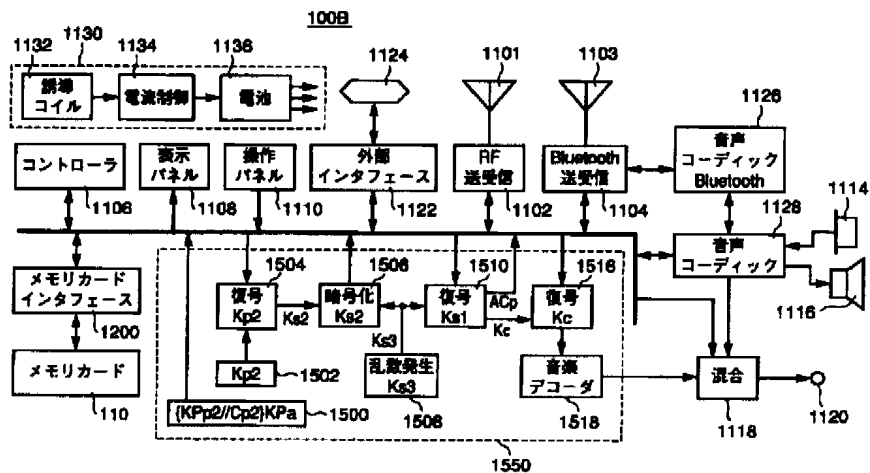
【図17】



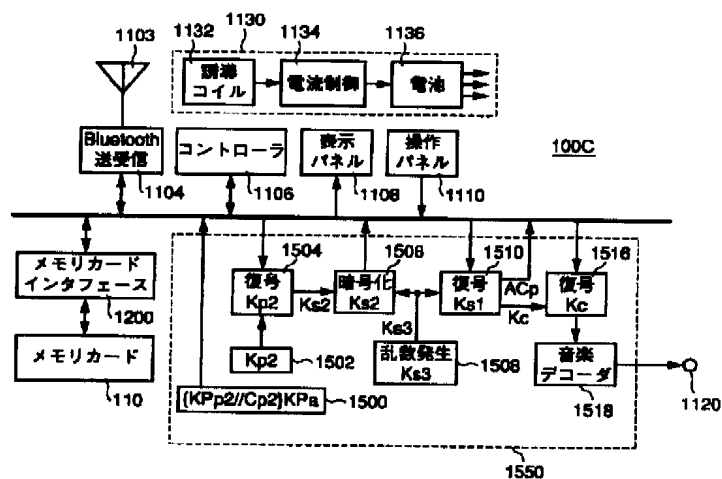
【図18】



【図19】



【图 20】



フロントページの続き

(51) Int. Cl. <sup>7</sup>

識別記号

FI

テーマコート<sup>®</sup> (参考)

H O 4 L 9/32

H O 4 N 7/16

$$Z$$

H 0 4 M 1/00

G 1 0 L 9/00

N

11/00

302

H O 4 L 9/00

6 0 1 A

H O 4 N 7/16

6 0 1 E

6 7 5 B

Fターム(参考) 5B017 AA06 BA09 CA00

5C064 BA07 BB02 BC03 BC04 BC06

BC17 BC18 BC22 BC23 BC25

BD02 BD03 BD04 BD08 BD09

CA14 CA16 CB01 CC01 CC04

5J104 AA07 AA15 AA16 EA06 EA18

KA02 KA05 NA02 NA03 NA35

NA37 NA38 NA41 PA02 PA11

5K027 AA11 BB09 CC08 FF28 HH24

HH29 KK02

5K101 KK18 LL12 NN07 NN15 NN21

UU19